United States Agency for International Development

Project Management Office Risk Management Plan

Final
MST-PMO-004-CP-017-F00-IBM

September 9, 2003

Prepared by:

Version History

Version	Publication Date	Description of Change	Author
v1.0	09/09/03	Initial issuance of Final	ama

TABLE OF CONTENTS

List of Tables

List of Figures

1 Summary

The United States Agency for International Development (USAID) initiated the Program Management Office (PMO) to assist the USAID Business Transformation Executive Committee (BETC) with support in forecasting, planning, managing, and monitoring business transformation and information technology projects. The PMO provides strategic planning, capital planning, project management, system development life cycle development and management, quality management, change management, business process improvements, and risk management.

A risk is an event that has not yet happened but, if it did, could threaten the successful outcome of a project or program. Risk management is the discipline that facilitates the achievement of project and program implementation goals by identifying threats to a project, assessing the nature of the threats, and defining and implementing actions that control these threats. Risk management is a continuous, forward- looking process that is an intricate part of the program management process.

To assist USAID in achieving its program and project goals, a risk management program, under the direction of the PMO, establishes the practice for performing risk management. The PMO Risk Management Plan (RMP) addresses an Agency need to institutionalize the risk management process at the project, PMO, and enterprise levels.

Specifically, the PMO RMP establishes the policy for identifying, analyzing, mitigating, and tracking of USAID risk at three distinct levels:

- Enterprise – consists of the Capital Planning and Investment Control (CPIC), BTEC and other governance bodies
- PMO – provides visibility into the progress of Business Transformation (BT) projects and works with the BTEC to monitor the performance of project investments
- Project – BT projects as established by the BTEC

The PMO RMP outlines the process to identify, analyze, document, and mitigate risks at the project, PMO, and enterprise levels. The PMO RMP focuses on the execution phase for managing project or program risks however; risks are acknowledged and managed prior to project or program startup.

Specifically, the PMO RMP documents:

- Standard procedures to support the identification and assessment of risks
- Standard procedures to support the development of mitigation/contingency plans
- Standard procedures to monitor and report risk status
- Measures for determining when actions are required for risk
- Standard tools for the tracking and management of risks

Successful implementation of the PMO RMP is dependent on the following factors:

- Roles and responsibilities are identified and funded to perform the risk management process
- Staff members and stakeholders are trained in the processes identified in the PMO RMP
- The identification and reporting of risks is encouraged and both the project, PMO and enterprise levels
- Authority and responsibility is assigned at the appropriate levels for the mitigation of risks
- Tools are available and implemented to support the risk management process

The PMO RMP was developed using the methodologies of Institute of Electronics and Electrical Engineers (IEEE) Std 1058-1998 for Software Project Management Plans, ANSI/PMI 99-001-2000 A Guide to the Project Management Body of Knowledge (PMBOK Guide) 2000 Edition, and the Capability Maturity Model Integration (CMMI) for Systems/Software Engineering v1.1.

2 Introduction

Risk Management is a process of the identification, measurement, control of risks, and financing of risk mitigation which threatens the achievement of program and project goals. As defined by the standards IEEE Std 1058-1998 for Software Project Management Plans, PMBOK for Project Risk Management, and CMMI for Systems/Software Engineering v1.1 for Risk Management, it is a best practice for the systematic planning, identification, analysis, and monitoring of risk.

IEEE Std 1058-1998 for Software Project Management Plans states that a risk management plan should:

- Identify, analyze, and prioritize project risk factors
- Describe the procedures for contingency planning
- Methods to be used in tracking risk factors
- Methods to be used in evaluating changes and response to changes

PMBOK for Project Risk Management identifies the following processes for risk management:

- Risk identification – determining which risks are likely to affect the project and documenting the characteristics of each
- Risk Quantification – evaluating risk and risk interactions to assess the range of possible project or program outcomes
- Risk Response Control – responding to changes in risk over the course of the project or program

CMMI for Systems/Software Engineering v1.1 at Maturity Level 3 is broken into the following specific goals for a risk management process:

- Prepare for Risk Management (determine risk, define risk parameters, establish risk strategy)
- Identify and Analyze Risks (identify, categorize, and prioritize risks)
- Mitigate Risk (develop and implement risk mitigation plans)

To manage risk at a project, PMO and enterprise level, the PMO RMP adopts the methodology and approach of IEEE, PMBOK and CMMI in the management of risk.

2.1 Background

Risk management is continuous, forward-looking process that provides management with the capability to be proactive rather than reactive. Risk management addresses issues that may endanger the achievement of program and project goals if they were to occur. A continuous risk management approach is therefore applied to anticipate and mitigate the risks that have a critical impact on program performance.

The PMO RMP documents the disciplines, definitions, roles and responsibilities, strategy, approach, processes, tools, and reporting that are used to manage USAID risk at an enterprise level. More specifically, it addresses an Agency immediate need to assign authority and responsibility for the review, validation, control, and reporting of risks.

2.2 Purpose

The purpose of the PMO RMP is to provide USAID Executive Sponsors, BT Project Managers, and Governance Bodies with processes and information to make informed decisions regarding project and program alternatives. The PMO RMP also provides a framework which encourages teams to take appropriate measures to minimize adverse impacts to scope, cost, and schedule.

2.3 Scope

The PMO RMP establishes the framework for the PMO risk management program. The plan outlines the processes to identify, analyze, document, mitigate, and monitor events that might adversely affect USAID project and program performance.

The specific goals of the PMO risk management program are:

- Assign specific responsibilities for the management of risk and prescribe the monitoring and reporting processes to be followed
- Serve as a basis for assessing, planning and controlling risks through identification, documentation, analysis, prioritization, and development of mitigation strategies
- Allow for the monitoring of the USAID project and program performance
- Assist USAID team members in making decisions regarding budget, resources, and schedule

The PMO Risk Lead develops and maintains the guidelines, procedures, and tools to support the processes defined in the PMO RMP.

2.4 Assumptions

The following assumptions were made in the development of this plan:

- On an periodic basis, individual projects will review and update their risk management plans to follow the procedures, guidelines, and standards established by the PMO RMP
- Projects are responsible for instituting a risk management program at the project level
- Risk Radar v3.2.4 is the tool that is used to manage, track, control, and report risk on the USAID BT program
- The procedures and templates noted in the appendices will be managed and maintained as separate living documents accessible from a common directory

2.5 References

The following documents were referenced in the development of the PMO RMP:

- Draft USAID Program Management Office Guidebook, version 1.0, dated November 8, 2003
- ADS 577- Information Technology Capital Planning and Investment Control, version 1.5, dated July 9, 2003
- IEEE Std 1058-1998 for Software Project Management Plans, dated December 8, 1998
- PMBOK for Project Management, dated 2000
- CMU/SEI-2002-TR-002 CMMI for Systems Engineering/Software Engineering Staged Representation, version1.1, dated December 2001

3 Roles and Responsibilities

Risk management serves to identify potential problems before they occur, so that risk-handling activities may be planned and invoked as needed to mitigate adverse impacts on achieving USAID program and project goals. It is an integrated team activity that requires the participation of team members across organizational boundaries. Members across the team share a stake in the achievement of USAID program and project goals. Stakeholders in the PMO risk management program are defined by roles that are described in this section.

3.1 Organization and Information Flow

The PMO RMP establishes an organizational framework for the management of risks. At the project level the risk management process provides projects with procedures and forms that are to be implemented at the project level. The PMO risk management program also provides BT projects with initial assistance for training and initiating the risk management process. At the PMO level, the risk management process identifies, tracks, and reports PMO risks and interacts with governance bodies and key stakeholders for reporting and mitigation of program risks. Figure 1: PMO Risk Management Organization and Information Flow depicts the flow of information between teams within the PMO program.

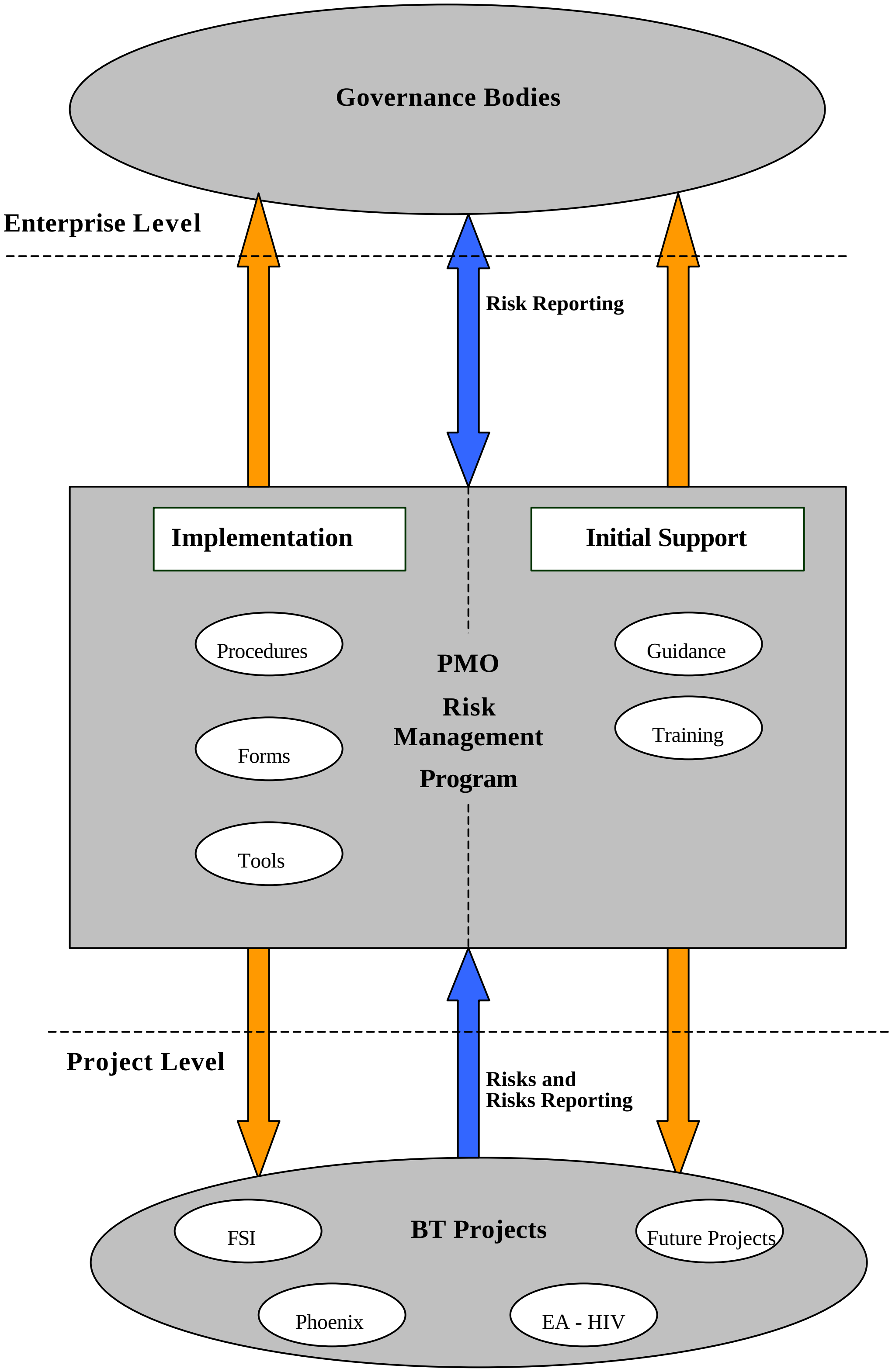


Figure 1: PMO Risk Management Organization and Information Flow

3.2 Governance Bodies

Governance Bodies consist of key stakeholders and participants at the enterprise levels. The PMO risk management program interacts with Governance Bodies with risk reporting to support the procurement, management, budgeting, and strategic planning of information technology investments.

Specific responsibilities are:

- Champion and communicate project goals and efforts to the enterprise organization and external stakeholders
- Forecast risks from external sources and cross-project dynamics
- Resolve issues evaluated from lower levels within the organization

3.3 PMO Risk Management Lead

The PMO RML facilitates the risk management process at three levels. At the project level, the PMO RML provides initial guidance and training to projects in the implementation of a risk management process. At the PMO level, the PMO Risk Lead manages, tracks, and reports PMO risks to program management. At the enterprise level, the PMO RML periodically reports risks of interest to governance bodies and other key stakeholders.

Specific responsibilities are:

- Manage the PMO risk management process, procedures, and tools
- Validate and manage PMO risks and monitor project and enterprise risks that the PMO is tracking
- Act as a point of contact for the project level RML
- Facilitate risk identification, analysis, and review sessions with projects
- Provide initial risk management training and guidance to project and program level team members
- Consolidate monthly project reports to produce a summarized dashboard report for project risks
- Confer with subject matters experts for the validation of PMO risk, as appropriate
- Communicate the status of PMO risk, and enterprise or project risks that the PMO is tracking, through the preparation and distribution of risk reports
- Periodically review risk processes and procedures and make recommendations for improvement

3.4 Project Risk Management Lead

The Project Risk Management Lead (RML) facilitates the risk management process as established by the PMO at the project and team levels. The Project RML enters risks into the risk database for validation by the Team Lead or Enterprise Architecture (EA) Project Manager.

Specific responsibilities are:

- Validate and manage project level risks and team risks
- Communicate project level risks and team risks through the preparation and distribution of risks reports
- Manage project risk management process, procedures, and tools
- Act as a point of contact for team leads in risk management activities
- Facilitate risk identification and review sessions with team leads and program management
- Provide risk management guidance to team members and team leads
- Produce a summarized dashboard report for risks
- Act as a point of contact for the PMO RML

3.5 PMO Manager

The PMO Manager assists in the implementation and management the PMO risk management program by providing guidance and oversight PMO staff.

Specific responsibilities are:

- Act as a point of contact for Executive Sponsors and Governance Bodies
- Interacts with the PMO RML in the identification and mitigation of PMO risks
- Participate in risk review meetings and the PMO and enterprise level, as appropriate
- Escalate project/PMO risk to the enterprise level, as appropriate

3.6 BT Project Manager

The BT Project Manager has overall responsibility for managing project risk. The implementation and execution of the risk management process as established by the PMO and escalation of risks are examples of BT project manager responsibility.

Specific responsibilities are:

- Assign risk owners to identified risk
- Works with the Project RML in the validation of identified risk
- Identify risk reserves needed for mitigation efforts
- Interface with the PMO RML, as required
- Maintain a project risk management plan
- Escalate project risk to the PMO and enterprise levels, as appropriate
- Reviews mitigation/contingency plans to validate that they are cost-effective and feasible
- Address and complete the risk section of the OMB Circular No. A-11 Exhibit 300

3.7 PMO Quality Assurance Lead/Project Quality Assurance Lead

The PMO Quality Assurance (QA) Lead and the Project QA Lead share the dual role to identify and report risks associated with the performance of quality control activities as defined in the PMO Quality Control Plan.

3.8 Risk Owner

The risk owner is responsible person for managing assigned risk. The risk owner defines the risk by completing the risk identification form in Attachment 1: Risk Identification Form. The risk owner then forwards the risk to the Project Manger/PMO RML for validation.

The risk owner defines the risk in terms of the following standard guidelines:

- Impact to the project, PMO or Agency
- Probability of occurring
- Impact timeframe for the risk

After the risk has been validated and entered into the risk database, the risk owner is responsible for developing a mitigation plan and contingency plan for the risk as appropriate. Risk owners have the primary responsibility for updating and maintaining assigned risks in the risk database.

3.9 Project Team Members

Members of a project team are responsible for taking an active role in the risk management process for their project or program areas. Team members support the risk management process in terms of the following:

- Identify risks

- Participate in risk review activities
- Participate in activities to mitigate risk

4 Risk Management Strategy and Approach

The PMO RMP contains a set of procedures, tools, and a uniform approach for the identification, assessment, and tracking of risks. The key elements of the risk management strategy and approach are listed in the following sections.

4.1 Methodology

As previous stated, the combination of elements from IEEE Std 1058-1998, PMBOK, and CMMI are used to form the methodology applied to the PMO risk management program.

The methodology establishes the following:

- Guidelines for risk planning
- Standard procedures to support risk identification and assessment
- Standard procedures to monitor and report risk status
- Measures for determining when actions are required for risk
- Standard tools for the tracking and management of risks

4.2 Risk Organization

Risk are organized, managed, and tracked at three levels, at the project level, the PMO level, and the enterprise level The risk management process, as detailed in Section 5, is implemented at all three levels for the identification, analysis, control, and monitoring of risks. To support the institutionalization of a PMO risk management process, the PMO RMP implements the risk categories established the OMB Circular No. A-11 Exhibit 300s. The categories are listed in Appendix F: Risk Categories.

4.3 Risk Thresholds

Risks that have a medium or high priority required immediate action for mitigation/contingency planning. Risk Radar, as the tool to manage USAID risk, automatically assigns a priority to the risk based on the potential impact and probability of the risk occurring. As detailed in Section 5.2.1, high and medium priority risks require management focus. High priority risks are considered to have greatest impact to project or program performance and therefore contingency planning is mandatory. Management reviews medium priority risk and decide if a contingency plan is warranted.

4.4 Mitigation Techniques

The PMO RMP establishes planning strategies for the mitigation of risks. The BT Project Manager and team member review risks and decide on the strategy that should be implemented for the risk.

The planning strategies to consider are:

- Risk Avoidance
- Risk Transference
- Risk Acceptance
- Risk Mitigation

Additional information on mitigation strategies may be found in Section 5.2.1.

4.5 Risk Measures

A measure is an operation of assigning a number to something. When a measure is applied, the resulting number obtained is a measurement. A metric is an interpretation of the assigned number. For example, if the height of a person is taken and the total number of inches is noted, the process is a measure and the number obtained is a measurement. The interpretation of the number as the person's height is a metric.

Examples of risks metrics include volatility and duration. A measure that supports a risk metric is called a risk measure.

The PMO risk management program establishes volatility and duration as the risks metrics to monitor risk impacts, the status of mitigation/contingency efforts, and the identification of new risks. The measures which supports the risks metrics is as follows:

- Volatility
  - Total number of Change Requests submitted for a reporting period impacting schedule or cost
  - Total number of earned value measurements exceeding targets by 10% for a reporting period
- Duration
  - Total number of new risk identified for a reporting period
  - Total number of risk with mitigation/contingency plans past due
  - Total number of High, Medium and Low priority risks for a reporting period

Sample reports from Risk Radar which support some of the risk measures above are displayed in Appendix E: Risk Radar Sample Reports.

4.6 Monitoring Intervals

The monitoring of risk is implemented at both the program level and the project level. At the project level, the project risks are reviewed at regularly scheduled team meetings. At these meetings, the status and mitigation/contingency efforts for risks are reviewed on a continuous basis. On a monthly basis, the RML completes the risk portion of the status report in Appendix D: Key to Success Sample Report. At the program level, the status and mitigation/contingency efforts for medium and high priority risks are reviewed at regularly scheduled program management meetings. On a monthly basis, the PMO RML summarizes the risk from individual Key to Success status reports to produce an integrated report for program management.

4.7 Tools

To assist in the tracking and management of identified risks, an automate risk tracking is used. The system is deployed using Risk Radar, a Microsoft Access-based application developed by the Software Program Managers Network. Risk Radar is a risk management database to help Executive Sponsors, BT Project Managers, and Governance Bodies with the ability to identify, prioritize, and communicate project, PMO and enterprise risks in a flexible and easy-to-use form.

Risk Radar provides standard database functions to add, change, and retire risks, and has specialized functions for prioritizing risks. The number of risks in each probability/impact category by time horizon is graphically displayed. Metrics reports provide the ability to view the status of activities cumulatively. Risk Radar also provides the capability to automatically sort risks and identify priority ranking.

The PMO RML and the Project RML uses Risk Radar to generate reports to report on the status of risks and mitigation efforts to Executive Sponsors, BT Project Managers, and Governance Bodies.

A set of sample reports from Risk Radar is located in Appendix E: Risk Radar Sample Reports.

5 Risk Management Process

The risk management process provides steps to assess, plan, and control risk. The process identified in Figure 2: Risk Management Process Steps, as followed, allows for the management of risks at the project, PMO, and enterprise levels. The risk management process is broken down into three stages: assess, plan, and control and illustrates the activities required to support the risk management process.

The following sections provide a description of the PMO risk management process stages and the steps supporting each process stage. Where roles are the same for the PMO RML and the Project RML, they are identified concurrently as "RML" with the assumption that the role is performed within the assigned PMO or project level unless otherwise specified. Procedures in the appendices detail the roles and steps that support the risk management process.

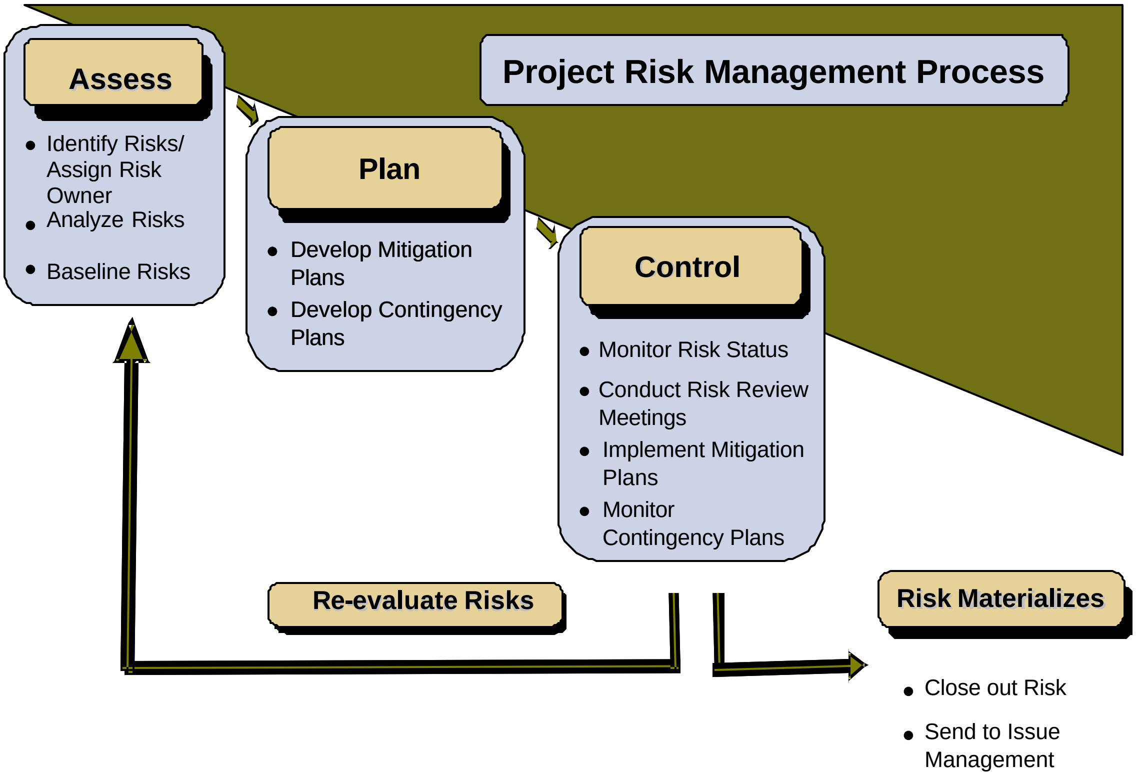

Project Risk Management Process
Assess
Identify Risks/ Assign Risk Owner
Analyze Risks
Baseline Risks
Plan
Develop Mitigation Plans
Develop Contingency Plans
Control
Monitor Risk Status
Conduct Risk Review Meetings
Implement Mitigation Plans
Monitor Contingency Plans
Re-evaluate Risks
Risk Materializes
Close out Risk
Send to Issue Management

Figure 2: Risk Management Process Steps

5.0 Define Project RMP

The initial step in the risk management process is the development of a project RMP and the assignment of roles. The establishment of project a project RMP is a requirement for BT projects. Refer to the USAID Program Management Office Guidebook for guidance on the development of a project RMP for BT projects.

5.1 Step 1: Risk Assessment

Risks are assessed throughout the life cycle of USAID projects. This process stage identifies potential risks and assigns probability, impact, and priorities for each risk. The procedure support the Risk Assessment process is located in Appendix A: Risk Assessment Procedure.

5.1.1 Risk Identification

The first step in the risk management process is risk identification. The early identification of risks across project and program areas is essential for the management of risks. Therefore, it is imperative that risk identification be planned, instituted, and continuous. Potential risks are identified at the start of a project, then continuously during life cycle phases or milestone events.

Examples of project and program risk triggers include the following:

- Cost or schedule variance is greater than 10% of the target (i.e. variance in earned value measurements or missed milestone targets in the work breakdown structure)

- Changes in scope or requirements which impact the cost or schedule greater than 10%
- Lost of a Subject Matter Expert or Sponsor as a key resources

The Risk Identification Form in Attachment 1: Risk Identification Form is used by any project team member to identify risks for inclusion in the risk database.

5.1.1.1 Risk Identification Sessions

Risks are identified as a part of ongoing USAID BT activities. Risks are identified at the following regularly scheduled team meetings:

- Program Management Team Meetings
- PMO Team Lead Meetings
- Project Status Meetings
- CPIC Meetings

Risks are also identified and noted in the OMB 300s and during ad hoc meetings with team members, governance bodies, and other key stakeholders.

When risks are identified, each proposed risk is assigned to a risk owner. The risk owner refines the risk description, if necessary, and performs analysis for each assigned risk. Risks are identified on a continuous basis and can be identified by any staff member. Results of risk identification efforts (whether from team meetings or ad hoc identification from any project team member) is documented in the risk database.

5.1.1.2 Define Risk

Identified risks are defined in the following terms:

If <*condition*> **and** <*dependency*>, **then** <*impact*>

Condition: Triggering event under which the risk will materialize, i.e., change in scope, budget adjustments, change in schedule

Dependency: Reason for the project's dependence on the risk, i.e., what will happen if the risk occurs

Impact: Quantifiable and measurable impact of the realized risk

For example, **if** a team member conducting application configuration analysis on a specific process was to leave the project, **and** we lose our subject matter expertise, **then** it will take one month longer than estimated to complete the project configuration activities.

5.1.1.3 Assign Risk Category

Risks categories are used to classify identified risks to facilitate analysis and decision-making. To support and promote consistency across organizational boundaries, the PMO implements the OMB Circular No. A-11 Exhibit 300 risk categories established by the CPIC for the identification of risks. A list of these risk categories is located in Appendix F: Risk Categories. Risk categories may change over the project life cycle. As risk categories change, the RML is responsible for managing updates to the risk database at the project, PMO, and enterprise level along with any associated procedures, templates, and forms.

5.1.2 Analyze Risks

Risk owners are responsible for assessing the impact on the project, the probability of occurrence, and timing of risks. Impact can be realized in terms of system performance, quality, and functionality as well as in terms of project performance. Performing risk analysis involves the following steps.

5.1.2.1 Determine Impact of Risk

The risk owner assesses each risk in terms of its likely impact on the project by assigning a value of 1-5 as defined in Table 1: Impact Definitions.

Table 1: Impact Definitions

Value	Rating	Description
1	Very Low	Likely to cause very minor delays or minimal additional work (or minimal degradation of system performance) that could be accomplished within existing constraints
2	Low	Likely to cause some delays or additional work (or low degradation of system performance) that may slightly exceed existing constraints, with a possible adverse impact on the project s chedule and resource requirement
3	Moderate	Likely to cause delays or additional work (or moderate degradation to system performance) that would exceed existing constraints, resulting in exceeded time scales, additional resource and/or additional budget requirements
4	High	Likely to cause significant disruption to the project (or significant degradation to system performance), resulting in the need to conduct re-planning and re-estimating
5	Very High	Likely to cause very significant disruption to the project (or very significant degradation to system performance), and could even result in failure of the project

5.1.2.2 Determine Probability of Risk

The risk owner assigns a value to the probability that the risk will occur during a given timeframe (in percentage). The values for the probability are based on the criteria defined below. Values range from 1 percent (extremely unlikely) to 99 percent (almost certain). The percentage is based on professional judgment and past experience. Table 2: Probability Definitions describes the probability definitions.

Table 2: Probability Definitions

Value	**Probability**	**Explanation**
70 – 99%	High	Very to likely to occur
30 – 70%	Medium	Likely to occur
1 – 30%	Low	Not likely to occur

5.1.2.3 Determine Occurrence of Risk

The risk owner identifies the time period when action is required to avoid or mitigate a risk. The risk owner identifies the earliest and latest date the risk could materialize. The impact horizon is presented in Table 3: Timeframe Definitions.

Table 3: Timeframe Definitions

Timeframe	Explanation
Near-term	Less than 30 days
Mid-term	30 - 90 days
Far-term	Greater than 90 days

5.1.2.4 Prioritize the Risk

The risk database automatically assigns a priority to a risk based on the potential impact and probability of the risk occurring. The priority assigned to a risk may change if the probability of its occurrence or its impact changes. Higher priority risks are to be monitored more closely are require the development of mitigation strategies and contingency plans.

Figure 3: Risk Assessment Matrix below displays a risk assessment matrix, indicating risks that portray a high probability of occurrence and a high level of impact are risks that require proactive responses.

Risk in the shaded areas has a high probability of occurring with the greatest impact. The development of mitigation strategies and contingency plans is required for Risk 1 and Risk 2. The development of mitigation strategies and contingency plans is encouraged for Risk 3 and Risk 4. Risks 5, 6, 7 and 8 are continually monitored and assessed until a determination is made that the risk has no probability of occurring, is no longer applicable, or poses no threat to project or program performance. If risk re-assessment results a change in priority to medium or high, mitigation or contingency plans are developed as described above.

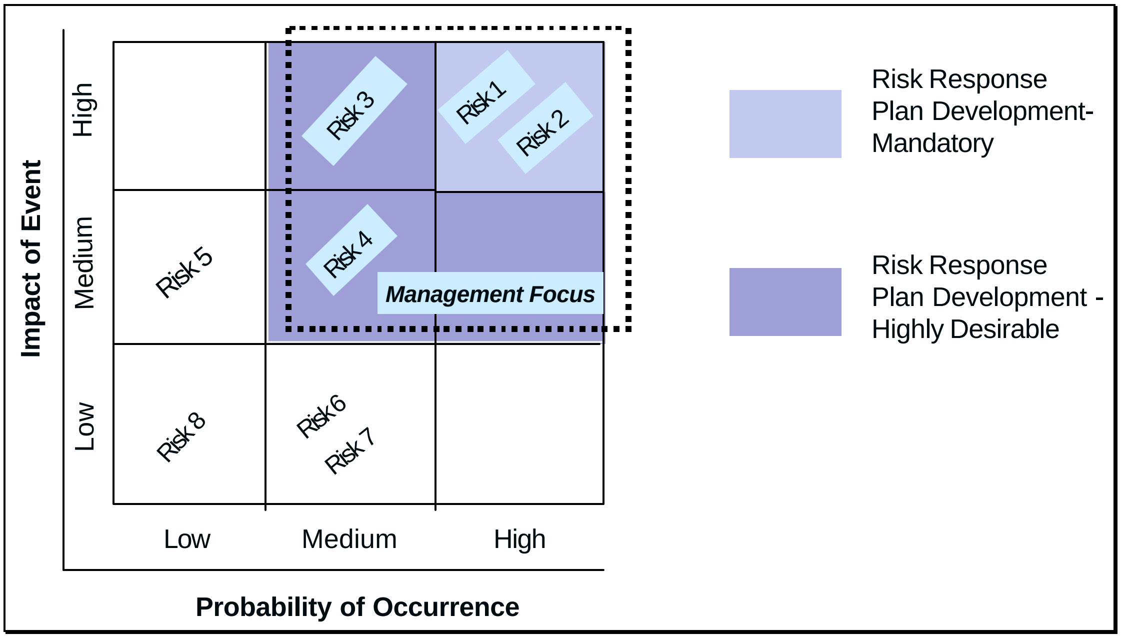

Impact of Event
High
Medium
Low
Risk 3
Risk 1
Risk 2
Risk 5
Risk 4
Management Focus
Risk 8
Risk 6
Risk 7
Low
Medium
High
Probability of Occurrence
Risk Response Plan Development- Mandatory
Risk Response Plan Development - Highly Desirable

Figure 3: Risk Assessment Matrix

5.1.2.5 Validate the Risk

Once the risk owner completes the risk analysis, the RML is responsible for working with subject matter experts to validate the risk. In validating the risk, the RML:

- Confirms that the risk element is a veritable threat to the project or program
- Agrees that the risk identification statement concisely provides a condition, impact and consequence
- Concurs with impact and probability measurements attributes
- Concurs with the reasonableness of anticipated period of occurrence

The validation of risk is based on the experience of subject matter experts. An identified risk that is not validated, based on result of its analysis, is closed out and not tracked or managed. The RML may request that the risk owner further refine the risk definition or perform additional analysis, if needed, to complete assessment activities.

If a risk materializes and is classified as an issue, the risk owner closes out the risk and transfers it to the issue management process. An issue owner is assigned to execute action plans and resolution activities to the closure of the issue.

5.1.3 Baseline Risks

When the RML determines that the risk description, triggering event, and metrics to be used to monitor for triggers are valid, the risk is considered baselined and is entered into the risk database. Reports for baselined risks are generated from Risk Radar by the RML as required for the monitoring and reporting of risk at the project, PMO, and enterprise levels.

5.2 Step 2: Risk Response

Following the Assess stage, the risk owner documents the activities that are used to manage each risk. The steps within this stage are:

- Develop risk avoidance or mitigation plans for medium and high priority risks
- Develop contingency plans for high priority risks
- Define metrics needed to track the status of the risks

The procedure support the risk response process is located in Appendix B: Risk Response Procedure.

5.2.1 Develop Mitigation Plans

Risk owners develop mitigation strategies for medium and high priority risks. Risk owners are required to complete mitigation plans within **one week** after the risk has been validated. The RML works with the risk owners to establish responsive mitigation plans. The mitigation plans takes into consideration the estimated cost of activities and proposed schedule to implement. Mitigation plans are reviewed by the PMO Manager/BT Project Manager to validate that the plan is cost-effective and feasible. Activity plans necessary to mitigate or lessen the risk consists of one or more of the following strategies:

- **Risk Avoidance:** Make plan changes to eliminate the risk or to protect project or program objectives from its impact. An example is a change in scope or the addition of resources to avoid or eliminate the risk.
- **Risk Transference:** Transfer responsibility and ownership of the risk to an outside resource or organization that has expertise in taking the steps to reduce the risks it occurs. An example is contracting out a scope of to a contractor who is skilled in taking the necessary steps to reduce the risks.
- **Risk Acceptance:** Acknowledge the existence of the risk and accept its consequences if it occurs. An example is the acceptance of schedule or cost overrun and developing a contingency plan to execute if the risk occurs.
- **Risk Mitigation:** Incorporate the ongoing monitoring and handling of risks throughout the life of the project or program. These mechanisms involve the use of reviews, possibly adding milestones, and development of counter measures and cost estimates. An example is the introduction of new processes or procedures to lessen the probability producing a defective product.

Risk owners specify the following in their mitigation plans:

- A plan of specific activities necessary to eliminate or reduce the likelihood or probability of the risk
- Team members responsible for implementing the plan, if different than the risk owner
- Triggering events that will prompt the implementation of the contingency plan
- Cost estimates for risk reserves to finance the implementation of mitigation efforts

The risk owner documents the mitigation plan in the risk database and tracks the progress of mitigation plan activities. Triggering events for risk are monitored and reported at monthly risk review meetings as discussed in Section 5.3.2.

5.2.2 Develop Contingency Plans

The PMO risk management process requires that risk owners develop contingency plans for high priority risks. Risk owners are required to complete contingency plans within **two weeks** after the risk has been validated. The PMO Manager/BT Project Manager determines if contingency plans are required for selected medium priority risks. Contingency plans are reviewed by the PMO Manager/BT Project Manager to validate that the plan is cost-effective and feasible.

Contingency plans are documented in the risk database by the risk owner. The contingency plan specifies the following:

- A plan of specific activities that are to be executed if the triggering event(s) occur
- Team members responsible for implementing the plan, if different than the risk owner
- Triggering events that will prompt the implementation of the contingency plan
- Cost estimates for risk reserves to finance the implementation of contingency efforts

The risk owner reviews contingency plans with the RML for practicality, cost-effectiveness, and appropriateness. Triggering events for risk are monitored and reported at monthly risk review meetings as discussed in Section 5.3.2.

5.3 Stage 3: Risk Control

The control stage involves careful monitoring of the status and evolution of identified risks and taking appropriate measures to minimize the impact of a risk when it materializes. These measures are based on the risk mitigation or contingency plans developed in previous steps. The steps that comprise the control stage consists of the regular monitoring of risk measures and triggering events, conducting periodic meetings to review risk status, implementation of defined mitigation plans, and implementation of contingency plans if triggering events occur.

Risk owners are responsible for the development and monitoring of mitigation plan steps that primarily comprise the risk control efforts. The RML reviews the status and progress of mitigation of high and medium priority risks on a monthly basis.

The procedure support the risk control process is located in Appendix C: Risk Control Procedure.

5.3.1 Monitor Risk Status

Risk owners monitor risks using Risk Radar as the tool to manage risk. Monthly reports from Risk Radar are generated and posted to provide visibility to project team members for monitoring of risk status. Risk owners re-assess and revise the probability, impact, and priority of the risks on an ongoing basis.

If the risk owner determines that a risk has no probability of occurring, is no longer applicable, or has been successfully mitigated, then the RML discusses closing or retiring the risk at the appropriate review meeting. The risk owner updates any changes to the risk status in Risk Radar. The RML is responsible for validating proposed changes to risks prior to database update.

5.3.2 Conduct Risk Review Meetings

The risk management process encourages project-wide and program-wide participation in the identification and mitigation of risks. The RML establishes monthly risk review meetings to review active risks, their status, mitigation progress, and proposed contingency plans.

The review of risks focuses on high priority risks and their strategies and plans developed by the risk owners. At risk reviews, the RML also makes recommendations to improve the effectiveness, priority, or progress of mitigation and contingency plans. Prior to reviews, the RML prepares summary information from Risk Radar and gather relevant updates from risk owners regarding their progress on mitigation and contingency planning activities.

As a review item, an anticipated review discussion for risk covers:

- Review of actions related to previously assigned risk
- Discussion of existing risks/plans with a priority of medium or high priority
- Review status of implemented mitigation/contingency plans
- Cost estimations or risk reserves for implementing mitigation/contingency plans
- Review of triggering events for continued validity and responsiveness
- Discussion, identification, and assignment of new risks
- Discussion of candidate risks for retirement or closure

5.3.3 Implement Mitigation Plans

Team members implement mitigation strategies for high and medium priority risks, as validated by the RML. The risk owner documents mitigation plans in Risk Radar and updates associated project documentation accordingly. The risk owner notifies the RML of any updates or changes to mitigation plans. Risk owners are responsible for working with their RML to update applicable project documents with changes to estimates, approach, resources, or schedules. The risk owner coordinates implementation of the mitigation strategy and provides progress updates to the RML. The RML monitors mitigation efforts to assess if the strategies are producing the desired results. The RML may recommend improvements to the risk to increase effectiveness of mitigation actions.

5.3.4 Implement Contingency Plans

High risks that materialize are accompanied by an associated contingency plan. The risk is closed in Risk Radar and is transferred to the issue management process. As an issue, project and program management review and consider executing the contingency plan that was developed under the risk management process. The assigned issue owner has the responsibility for implementing the contingency plans as reviewed by project and program management.

5.3.5 Risk Escalation

During the life cycle of the BT program, risks may arise which require attention at high levels within the Agency. Risks are escalated for medium or high priority risk when there is a potential impact across projects or there is a potential adverse impact to BTEC IT investments. The PMO Manager/BT Project Manager has the primary responsibility for the escalation of risks to the appropriate PMO and enterprise levels. Medium or high priority risk with the potential to impact BTEC IT investments are escalated at the enterprise level for visibility and control. Medium or high priority risk with the potential to cross-project impact, are escalated at the PMO level for visibility and control. The PMO Manager will determine if cross-project impact risk require escalation to the enterprise level.

6 Risk Reporting

Three types of risk reporting are used to support the PMO risk management program:

- Risk reports from Risk Radar
- Monthly project status reports
- Monthly risk reports presented at project and program reviews

6.1 Risk Reports from Risk Radar

To promote the implementation of risk management process at the project, PMO, and enterprise levels, reports from Risk Radar, are generated and presented at monthly project and program risk meetings. Summary monthly risk reports are posted in a common directory for access for project and program teams. Sample reports from Risk Radar are included in Appendix E: Risk Radar Sample Reports.

6.2 Monthly Project Status Reports

At the project level, the Project RML completes the Keys to Success for monthly project status reporting. Quantitative and qualitative facts are compiled for each key area to arrive at red/yellow/green dashboard ratings. Risk is one of the key areas addressed in the Keys to Success assessment. Project RMLs provide their worksheets to the PMO RML for the generation of consolidated dashboard report. Consolidated dashboard reports are summarized and reported monthly to PMO and governance bodies status meetings. A sample dashboard report is located in Appendix D: Key to Success Sample Report.

6.3 Monthly Risk Reports

At the project level, the Project RML, collects and summarizes the project risks from the Monthly Keys Team Report and Risk Radar to produce an integrated report for project management. At the PMO level, the PMO RML collects and summarizes PMO risks, as well as project risks for medium and high priority risks, to produce an integrated report for program management. Monthly reports focus on the status of mitigation/contingency efforts for high priority risks.

Appendix A: Risk Assessment Procedure

1 Purpose

A risk is an event that has not happened but, if it did, could threaten the successful outcome of an event. Assessment is required to evaluate if the identified risk poses a viable threat to program and project goals. This procedure outlines steps to identifying potential risks and records them for further analysis and mitigation.

Specific activities are:

- Generating risk statements in a prescribed manner concisely describing context, dependency, and impact to the programs and projects
- Assigning risk owners for further analysis, validation and mitigation planning
- Documenting identified risks in the risk database
- Conducting analysis of risk
- Developing mitigation and (if applicable) contingency plans

2 Roles and Responsibilities

Team members are required to identify and raise potential risks which may threaten the success of program and projects goals. The following represents the specific roles and responsibilities to support the risk assessment process:

Risk Owner

The risk owner defines the risk using the guidelines established in the PMO Risk Management Plan; assigns a risk category for risk, determines risk impact, probability occurrence, and timeframe when risk could materialize.

Risk Management Lead

The Risk Management Lead (RML) assigns owners to risk; reviews and validates risk at the appropriate PMO, project, and enterprise levels; and validates and approves risks for entry into the risk database.

Team Members

Team members identify and report project risks (i.e., potential threats to task, schedule or cost objectives) as a continuous forward looking activity throughout the life cycle of the program or project.

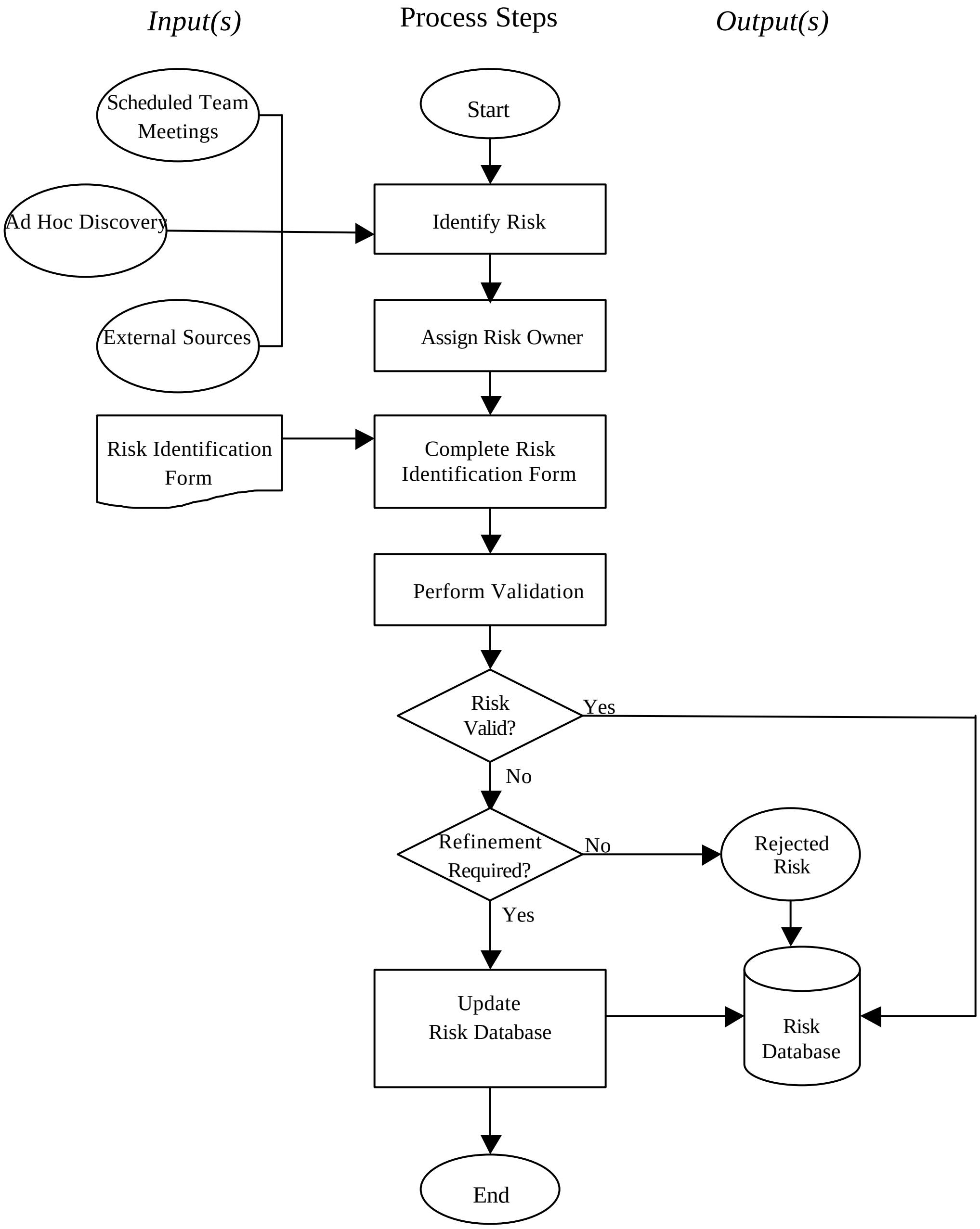
3 Prerequisites

The identification of risks is the prerequisite for executing this procedure.

4 Procedure Flow

The following diagram represents the process flow for the risk assessment process:

Figure A-1: Risk Assessment Process



5 Procedure Steps

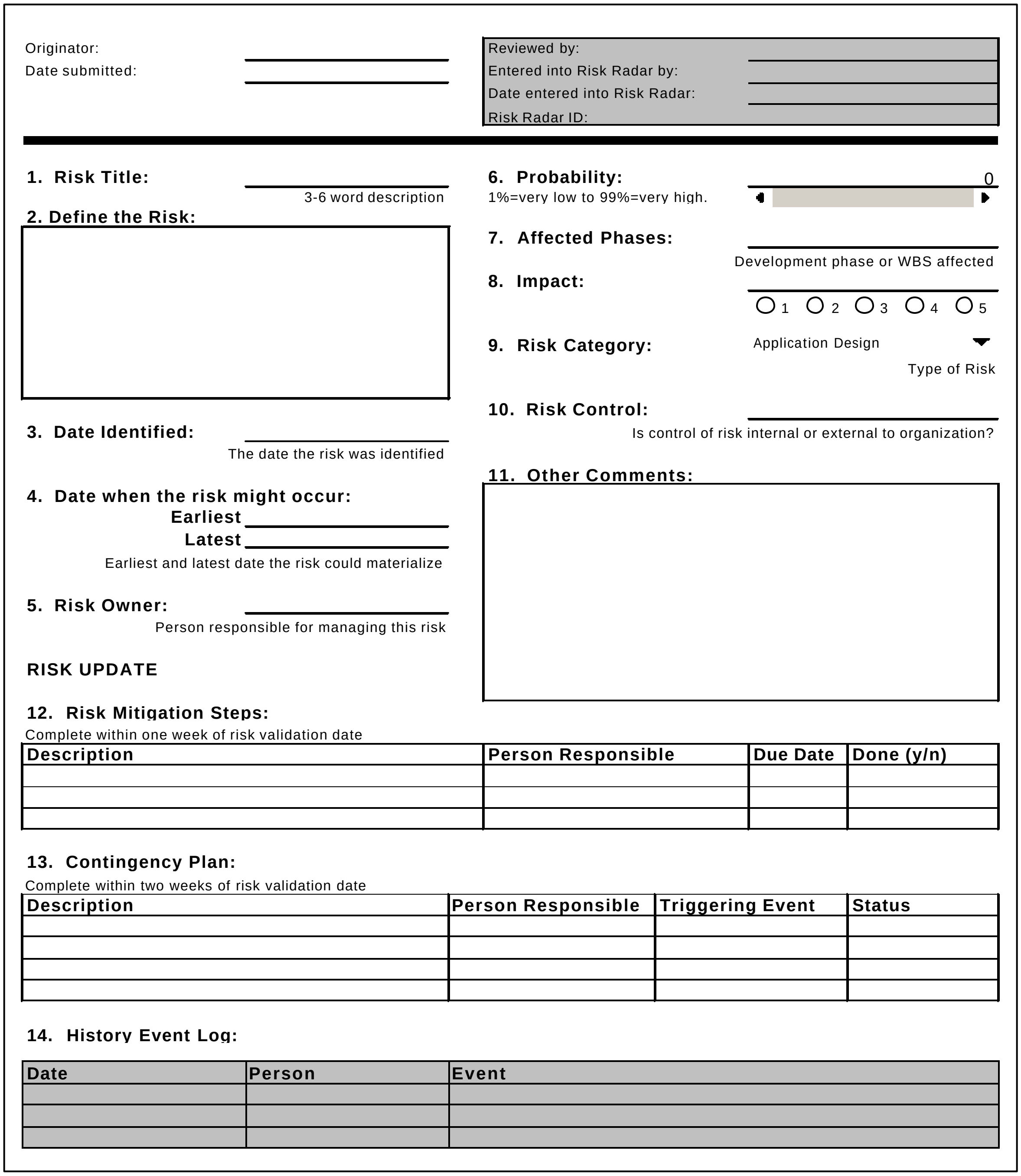
The following table documents the steps for conducting the deliverable review process:

Step	Description	Responsibility
1.	Identified potential risk which adversely affect one or more of the following: • Cost • Schedule • Scope Potential risks are identified as regular schedule team status meetings, ad hoc meetings, or from external sources.	Team Members
2.	Assign risk owner who is responsible for analyzing the risk in terms of impact, probability, and timeframe.	RML
3.	Define the risk by completing the identification form in Attachment 1. Forward the completed form to the RML within **3** business days of assignment.	Risk Owner
4.	Perform risk validation: • Confirm that risk is a veritable threat to the program or project • Agree the risk identification statement is accurate and clear • Concur with impact and probability measurement attributes • Concur with anticipated time period of occurrence	RML
5.	If it is determined that the risk is valid, it is maintained and tracked in the risk database.	Risk Owner
6.	If it is determined that the risk is not valid (rejected), the risk is closed by updating the status in the risk database. Note: The closed out risk will not be monitored or tracked.	Risk Owner
7.	If it is determined that the risk requires further information or additional analysis, responsibility is returned to the risk owner for refinement in the risk database.	Risk Owner

6 Procedure Output

The output produced by the execution of this procedure consists of risks which have been baselined in the risk database.

Attachment 1: Risk Identification Form



Originator: ____________

Date submitted: ____________

Reviewed by: ____________

Entered into Risk Radar by: ____________

Date entered into Risk Radar: ____________

Risk Radar ID:

1. Risk Title: ____________
3-6 word description

2. Define the Risk:

3. Date Identified: ____________
The date the risk was identified

4. Date when the risk might occur:
Earliest ____________
Latest ____________
Earliest and latest date the risk could materialize

5. Risk Owner: ____________
Person responsible for managing this risk

6. Probability: 0
1%=very low to 99%=very high.

7. Affected Phases: ____________
Development phase or WBS affected

8. Impact: ____________
○ 1 ○ 2 ○ 3 ○ 4 ○ 5

9. Risk Category: Application Design ▼
Type of Risk

10. Risk Control: ____________
Is control of risk internal or external to organization?

11. Other Comments:

RISK UPDATE

12. Risk Mitigation Steps:
Complete within one week of risk validation date

Description	Person Responsible	Due Date	Done (y/n)

13. Contingency Plan:
Complete within two weeks of risk validation date

Description	Person Responsible	Triggering Event	Status

14. History Event Log:

Date	Person	Event

1. Risk Title:

Create a brief 3-6 word description

2. Define the Risk:

Provide a brief definition in terms of the following structure:

If <*condition*> and <*dependency*>, then <*impact*>

Condition: Triggering event under which the risk will materialize
Dependency: Reason for the project's dependence on the risk; what will happen if the risk occurs
Impact: Quantifiable impact of the realized risk. What will happen if the risk occurs. Be as specific as possible, rather than using more general or anecdotal terms.

*Ex*ample: **If** a team member conducting application configuration analysis on a specific process were to leave the project **and** we lose our subject matter expertise, **then** it will take one month longer than estimated to complete the configuration activities necessary for conference room pilots.

3. Date Identified:

Enter the date risk was identified

4. Date when the risk might occur:

Identify the earliest and latest date the risk could materialize. ("BOP" can be used for beginning of project and "EOP" can be used for end of project.)

5. Risk Owner:

Identify the person that will be responsible for managing the risk

6. Probability of Risk:

Choose any number between 1 and 99%. The values below give an idea of ranges.

Value	Probability	Explanation
1 – 30%	Low	Not likely to occur
31 – 70%	Medium	Likely to occur
71 – 99%	High	Very to likely to occur

7. Impact of Risk:

Select: 1 (Very Low), 2 (Low), 3 (Moderate), 4 (High), 5 (Very High)

8. Affected Phases:

Development phase or WBS affected

9. Risk Category:

Types of risks include the following:

- Business – reliance of congressional and OMB approval of budgets
- Data/Info – replacement cost lost data/information, conversion cost of data/information
- Dependencies and Inter-operability – decisions regarding the BT projects and funding of implementation could impact performance goals
- Feasibility – functional requirements may not be met by baseline software
- Initial Cost – costs for initial deployment may exceed initial forecasts
- Investment Management Capability – program management may not be able to monitor and control schedule, costs, and risks for an investment
- Life-Cycle Costs – life-cycle costs for deployment may exceed initial forecasts
- Monopoly for Future Procurements – locked into a proprietary approach with no alternatives
- Organizational and Change Management – developing and implementing an approach that may require changes in processes, workflows and organizations
- Privacy – unauthorized access to sensitive data
- Project Resources – level of involvement of program management staff for support and availability of subject matter expertise
- Reliability of System – repository tools which may not support technical requirements
- Risk of Project Failure – dynamic requirements from oversight organizations, misunderstanding of capabilities and needs, lack of endorsement, support, and participation from senior management
- Schedule – ability to meet the schedule targets and goals
- Security – unauthorized access to operational systems
- Strategic – OMB or congressional approach and direction that may impact project goals
- Surety – protection of project and program assets
- Technology – consideration of evolving technology and ability to integrate current technology with future platforms
- Technical Obsolescence – technical approach will not evolve to support project or program requirements

10. Risk Control:

Is control of risk internal or external to the project or program? Or both?

11. Other Comments: (optional)

Use this field to provide any additional information, context, or rationale for selecting probability or impact assessments, financial risk reserves, etc.

12. Mitigation Plans:

Mitigation plans identify steps/actions that will be taken to eliminate or reduce the probability of a risk occurrence. Risk owners are required to create mitigation plans for high- and medium-priority risks. **Mitigation plans,** if required, **are to be completed one week after the risk has been validated.**

12. Risk Mitigation Steps:

complete within one week of risk validation

Description	Person Responsible	Due Date	Done (y/n)

Description: List steps/actions recommended to mitigate risk

Person Responsible: List a person for each step/action

Due Date: When should the person complete assigned step

Done (y/n): Current status of each step/action

13. Contingency Plans:

Contingency plans identify steps/actions that will be taken if the risk does occur. Risk owners are required to create contingency plans for high-priority risks only. Contingency **plans,** if required, **are to be completed one week after the risk has been validated.**

13. Contingency Plan:

complete within two weeks of risk validation

Description	Person Responsible	Triggering Event	Status

Description: List steps/actions recommended to mitigate risk

Person Responsible: List a person for each step/action

Triggering Event: What event would invoke the contingency plan

Status: Current status of each step/action

Appendix B: Risk Response Procedure

1 Purpose

After a risk has been identified, assessed, and prioritized, mitigation plans and contingency plans are developed for medium and high priority risk. Mitigation plans document the steps to be taken to avoid the risk and minimize the impact of the risk occurring. Contingency plans are required for high priority risk and addresses actions to be taken if a risk materializes.

This procedure outlines steps for the development and implementation of mitigation/contingency plans for validated risk.

2 Roles and Responsibilities

The following represents the roles and responsibilities required to support the execution of the risk planning process:

Risk Owner

The risk owner develops mitigation/contingency plans using the guidelines established in the PMO Risk Management Plan, and documents the resulting steps or actions that must take place to execute the mitigation/contingency plan.

PMO Manager/BT Project Manager

Reviews mitigation/contingency plans to assess the feasibility of proposed mitigation and contingency plans in terms of cost-effectiveness and feasibility for implementation.

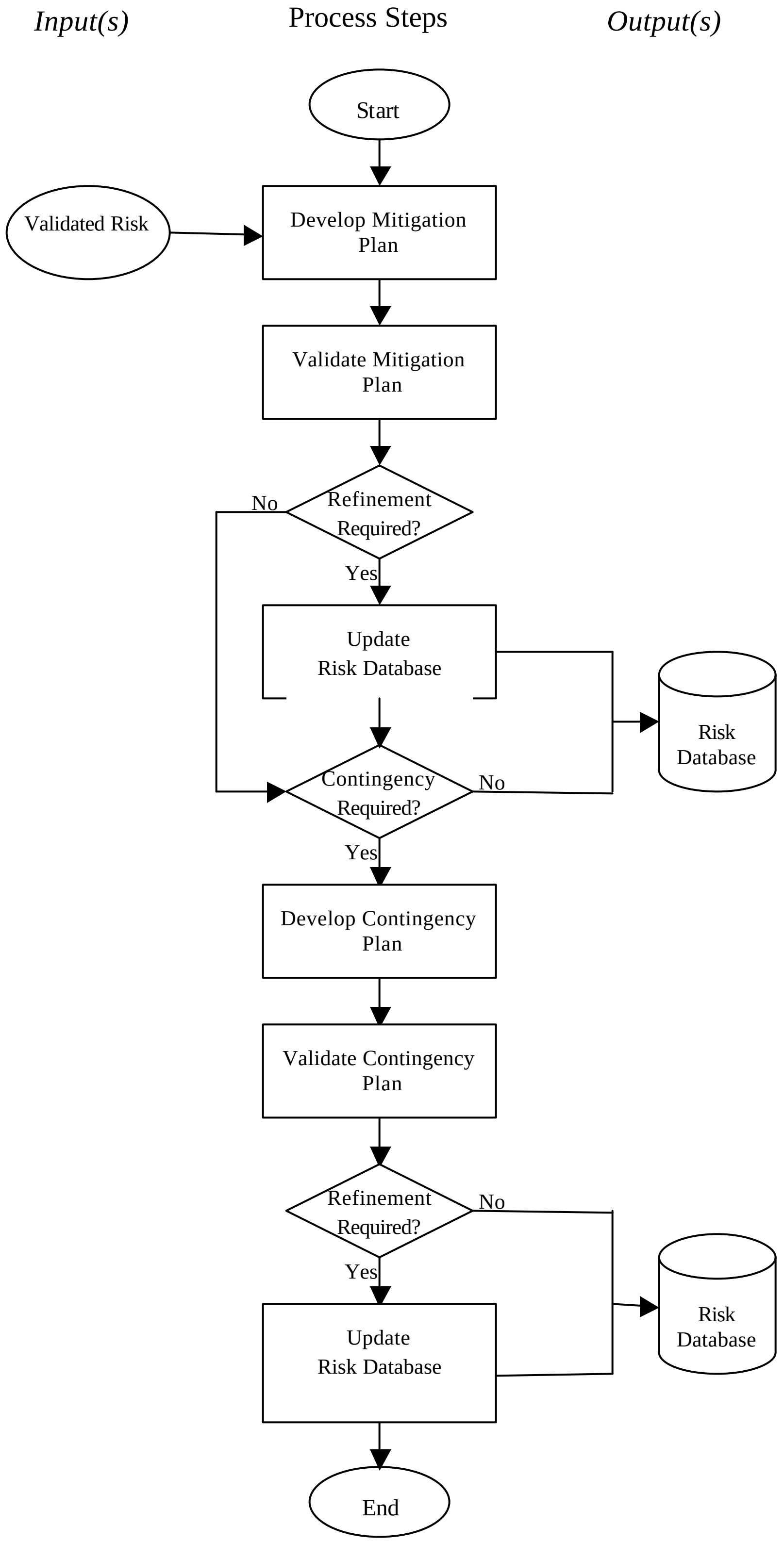
3 Prerequisites

A validated risk in the risk database is the prerequisite for executing this procedure.

4 Procedure Flow

The following diagram represents the process flow for the deliverable review process:

Figure B-1: Risk Response Process



5 Procedure Steps

The following table documents the steps for conducting the deliverable review process:

Step	Description	Responsibility
1.	Develop the mitigation plan for assigned risk with a medium and high priority. Develop the plan using one or more of the following strategies to mitigate or lessen the risk should it materialize: • **Risk Avoidance:** Make plan changes to eliminate the risk or to protect project or program objectives from its impact. An example is a change in scope or the addition of resources to avoid or eliminate the risk. • **Risk Transference:** Transfer responsibility and ownership of the risk to an outside resource or organization that has expertise in taking the steps to reduce the risks it occurs. An example is contracting out a scope of to a contractor who is skilled in taking the necessary steps to reduce the risks. • **Risk Acceptance:** Acknowledge the existence of the risk and accept its consequences if it occurs. An example is the acceptance of schedule or cost overrun and developing a contingency plan to execute should the risk occur. • **Risk Mitigation:** Incorporate the ongoing monitoring and handling of risks throughout the life of the project or program. These mechanisms involve the use of reviews, possibly adding milestones, and development of counter measures and cost estimates. An example is the introduction of new processes or procedures to lessen the probability producing a defective product. Develop the mitigation plan in terms of the following: • Specific activities necessary to eliminate or reduce the probability of the risk occurring • Assign responsibility to team members for implementing the plan, if different then the risk owner • Define the triggering events that will prompt the implementation of the contingency plan if the risk is a high priority risk • Estimate reserves needed to implement the plan if the risk occurs	Risk Owner
2.	Validate the mitigation plan by confirming that the plan takes into account considerations for the cost of activities (e.g risk reserves) and the proposed schedule for implementation. If it is determined that the mitigation plan requires further information or additional analysis, the risk owner is responsible for refining the risk in the risk database.	BT Project Manager/ PMO Manager

3.	If the risk is a high priority risk, the development of a contingency plan is required. If the risk is a medium priority risk, the PMO Risk Lead/Project determines if a contingency plan is required. Develop the mitigation plan in terms of the following: • Specific activities that are to be executed if the triggering event occurs • Assign responsibility to team members for implementing the plan, if different then the risk owner • Define the triggering events that will prompt the implementation of the contingency plan • Estimate reserves needed to implement the plan if the risk occurs	Risk Owner
4.	Validate the contingency plan by confirming that the plan is feasible and cost-effective. If it is determined that the contingency plan requires further information or additional analysis, the risk owner is responsible for refining the risk in the risk database.	BT Project Manager/ PMO Manager

6 Procedure Output

The output produced by the execution of this procedure is the entry/update of mitigation/contingency plans for risks.

Appendix C: Risk Control Procedure

1 Purpose

After mitigation/contingencies plans have been developed, careful monitoring of risk is required to minimize the impact if a risk materializes. The regular monitoring of risk metrics and triggering events, conducting periodic meetings to review the status of risks, the implementation of mitigation/contingency plans are specific examples. This procedure outlines the control process for the management risk.

Specific activities are:

- Monitor risk status
- Conduct risk review meetings
- Implement, track, and update mitigation plans, as appropriate
- Implement, track and update contingency plans, as appropriate

2 Roles and Responsibilities

The following represents the roles and responsibilities required to support the execution of the risk control process:

Risk Owner

The risk owner monitors and updates mitigation/contingency plans for assigned risks; monitors activities that trigger the implementation of a mitigation/contingency plan; coordinates implementation of resulting mitigation/contingency steps and activities; re-assess and revise the probability, impact, and priority of risk on a continuous basis; updates any changes to risk status in the risk database

PMO Manager/BT Project Manager

Reviews mitigation/contingency plans to assess the feasibility of proposed mitigation and contingency plans in terms of cost-effectiveness and feasibility for implementation.

Team Members

Team members participate in activities related to the review of risk and the implementation of mitigation/contingency plans.

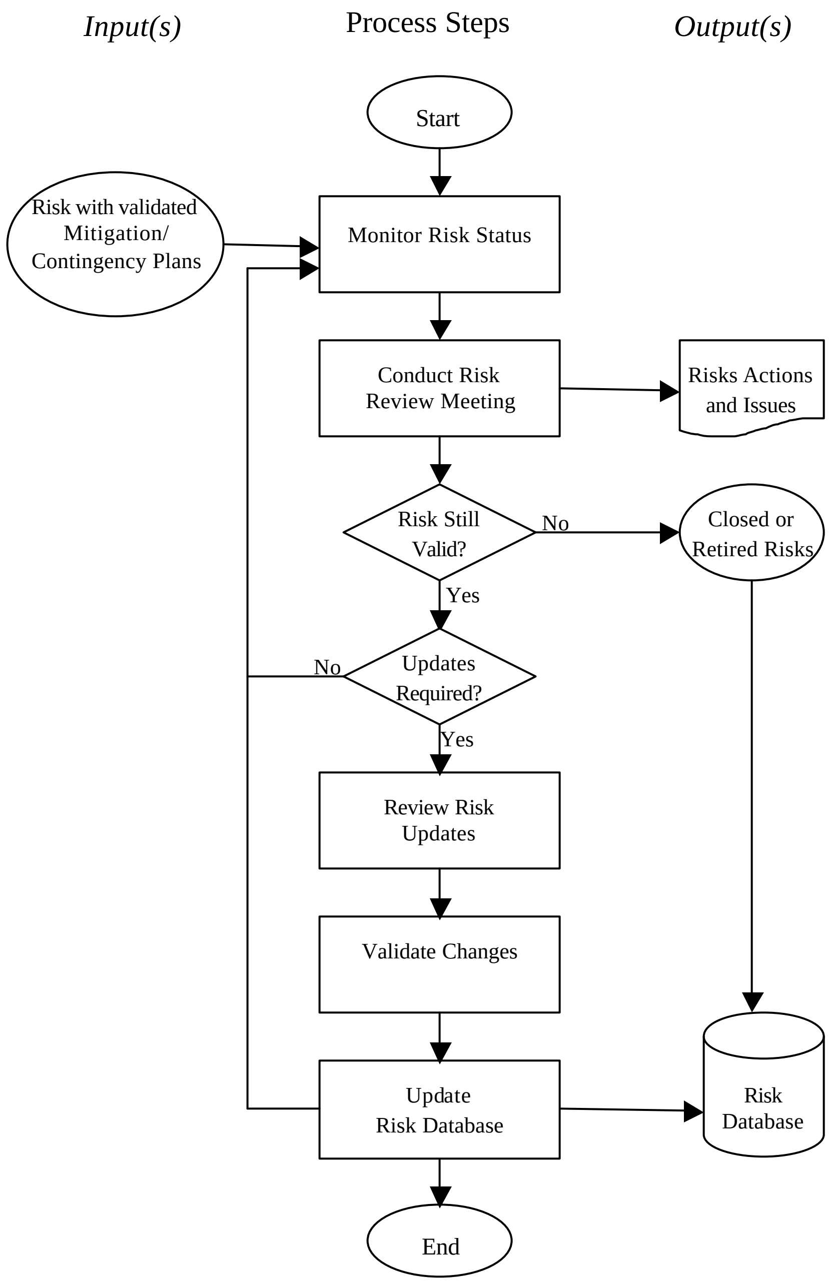
3 Prerequisites

A risk with a validated mitigation/contingency plan in the risk database is the prerequisite for executing this procedure.

4 Procedure Flow

The following diagram represents the process flow for the risk control process:

Figure C-1: Risk Control Process



5 Procedure Steps

The following table documents the steps for conducting the deliverable review process:

Step	Description	Responsibility
Ongoing	Monitor the status of risk using the risk database. Re-assess and revise the probability, impact, and priority of risks. Monitor triggering events which signal the implementation of mitigation/contingency plans. Coordinate activities for the implementation of mitigation/contingency steps.	Risk Owner
Ongoing	Monitor mitigation efforts to assess if the planned strategies are producing the desired results. Recommend improvements to increase effectiveness of mitigation strategy at the risk review meeting.	RML
1.	Conduct risk review meetings on a monthly basis to review the following: • Review of actions related to previously assigned risk • Review existing risks/plans with a priority of medium or high priority • Review status of implemented mitigation/contingency plans • Review, identify, and assign new risks • Review risks for retirement or closure • Review status of implemented mitigation/contingency plans • Document any actions/issues related to risk and post in the common directory.	RML
2.	Review proposed updates for mitigation/contingency plans in terms estimates, approach, resources, or schedules.	Risk Owner
3.	Validate proposed changes from risk review meeting in terms of cost, scope and schedule.	BT Project Manager/ PMO Manager
4.	Update validated changes to risk in the risk database.	Risk Owner

6 Procedure Output

The output produced by the execution of this procedure is the possible update of risk in the risk database and actions or issues from review meetings.

Appendix D: Key to Success Sample Report

Phoenix Rollout Monthly Team Report	Team Name: *Program Management* Lead Contractor: IBM Contractor Team Lead: Angela Carrington WBS Number: 1 As Of Date: 07/31/2003	**Summary Position** Green (G) – No Concerns Yellow (Y)– Potential Issues Red (R) – Significant Issues Grey – Not Currently Tracked	**Last period** □	**This period** Y

KEY ACCOMPLISHMENTS

1. Established PM Team WBS and Project Plan for pilots
2. Updated PM Team Charter and Phoenix Rollout Project Charter
3. Met with rollout teams to build Integrated Project Plan (IPP) for pilots

PLANNED ACTIVITIES

1. Draft attachments to WBS and IPP with cost and FTE estimates
2. Draft High-Level Deployment Strategy
3. Draft Mission Participation Requirements document

KEYS TO SUCCESS

	Last Period	This Period
1. Stakeholders Weekly meetings with David Ostermeyer (Acting CFO) and USAID counterparts.	□	G
2. Business Benefits to USAID The WBS and IPP will guide how USAID's financial system will be deployed to overseas missions.	□	G
3. Work and Schedule Deliverables for the PM team were on-time. Given the volume of work required for planning and start-up tasks, the team has been working well above 8 hours each day. The PMO is concerned because the WBS and IPP have not yet been finalized.	□	Y

WBS	Description	Baseline Schedule Date	Approved Changed Schedule Date	Actual Completion Date	Status
1.1.3.2	Work Breakdown Structure – Final	08/15/03	08/29/03		Y
1.1.4.2	Integrated Project Plan - Pilots – Final	08/15/03	08/29/03		Y
1.2.1.2	Risk Management Plan – Final	08/29/03			G
1.2.5.1.1	High-Level Deployment Strategy – Draft Final	08/22/03			G
1.2.5.1.2	High-Level Deployment Strategy – Final	08/29/03			G
1.3.1.2	Monthly EVM Reports - Final - July 03	08/21/03			G
1.4.1.1	Project Management Plan - Outline	07/16/03		7/16/03	G
1.4.1.2	Project Management Plan - Draft Final	08/27/03	9/19/03		🟩
1.5.1.1	Overseas Deployment OMB Exhibit 300 - Draft Final	07/31/03		7/31/03	G

4. Team & Infrastructure

Last Period	This Period
□	Y

The team is high-performing, but needs to have a dedicated EVMS person. Will need to assess and adjust level of staffing to support pilot rollout and full mission deployment.

5. Scope

□	Y

The scope of work for the PM team has been reviewed and agreed to by IBM and USAID contracting officers. Work to date has been in scope, but with a few “other reports” designations for ad-hoc requests. The PMO is concerned no finalized WBS is in place.

6. Risks

Resource Constraints (e.g., Continued OMB funding, other Agency funding constraints, direct hire and contractor staffing, direct hire participation on teams, etc.).
Impact of the election year.
Deliverable review and “sign off” approval process on key deliverables can be time consuming and can cause risk to completing milestones.
Roles of the contract vehicles and contractor staff need further definition.
Project scope needs further definition.
Schedule impacts and dependencies [e.g., viability of technical concept of operations due to bandwidth constraints and

latency issues, Department of State's decision regarding the Momentum version to be implemented, PMO guidance issued during project implementation, regionalization, PRIME recompete, and external oversight (OMB, Congress, Independent Validation and Verification contractors, IG, etc.)].
Process changes could cause negative view towards a new system in the field.
Data quality and migration issues could lead to users not being able to obtain the information they need from the system required for daily operations as well as decision making.
Increased security and privacy risks caused by implementing globally; when implementing globally, there is an increased risk of unauthorized access to the system.

7. Benefits to Phoenix Rollout Team

Draft final team and project charters, establishing roles, responsibilities, and KPI was completed.

Key Performance Indicators (KPI)	Last Period	This Period
Overall KPI Status	□	Y

KPI 1 Deliverables	Last Period	This Period
Measure: 95% of deliverables are completed on time.	□	G

KPI 2 Project Quality Standards & DRT	□	G

Measure: All project deliverables meet project quality standards and are approved via the project deliverable review process.

KPI 3 Project Budget

Measure: Overall project budget is within +-5% of baseline.

** The project budget has not been base-lined. Contractors are building cost estimates and FTE requirements.

KPI 4 EVMS	□	Y

Measure: A contractor earned value management system (EVMS) that supports both contractor and USAID performance management requirements is in place and operational.

** The project budget has not been base-lined. Contractors are building cost estimates and FTE requirements. The WBS and IPP have not been finalized.

□ G

KPI 5 Monthly Reports

Measure: Monthly reports are completed and submitted within 10 business days after end of month.

□ Y

KPI 6 EVMS Variance

Measure: EVMS variance at completion figures are within +-10% of the baseline plan.

** The project budget has not been base-lined. Contractors are building cost estimates and FTE requirements. The WBS and IPP have not been finalized.

□ G

KPI 7

Monthly Project Status Meetings

Measure: Monthly project status meetings are held with the Executive Sponsor (CFO).

□ Y

KPI 8

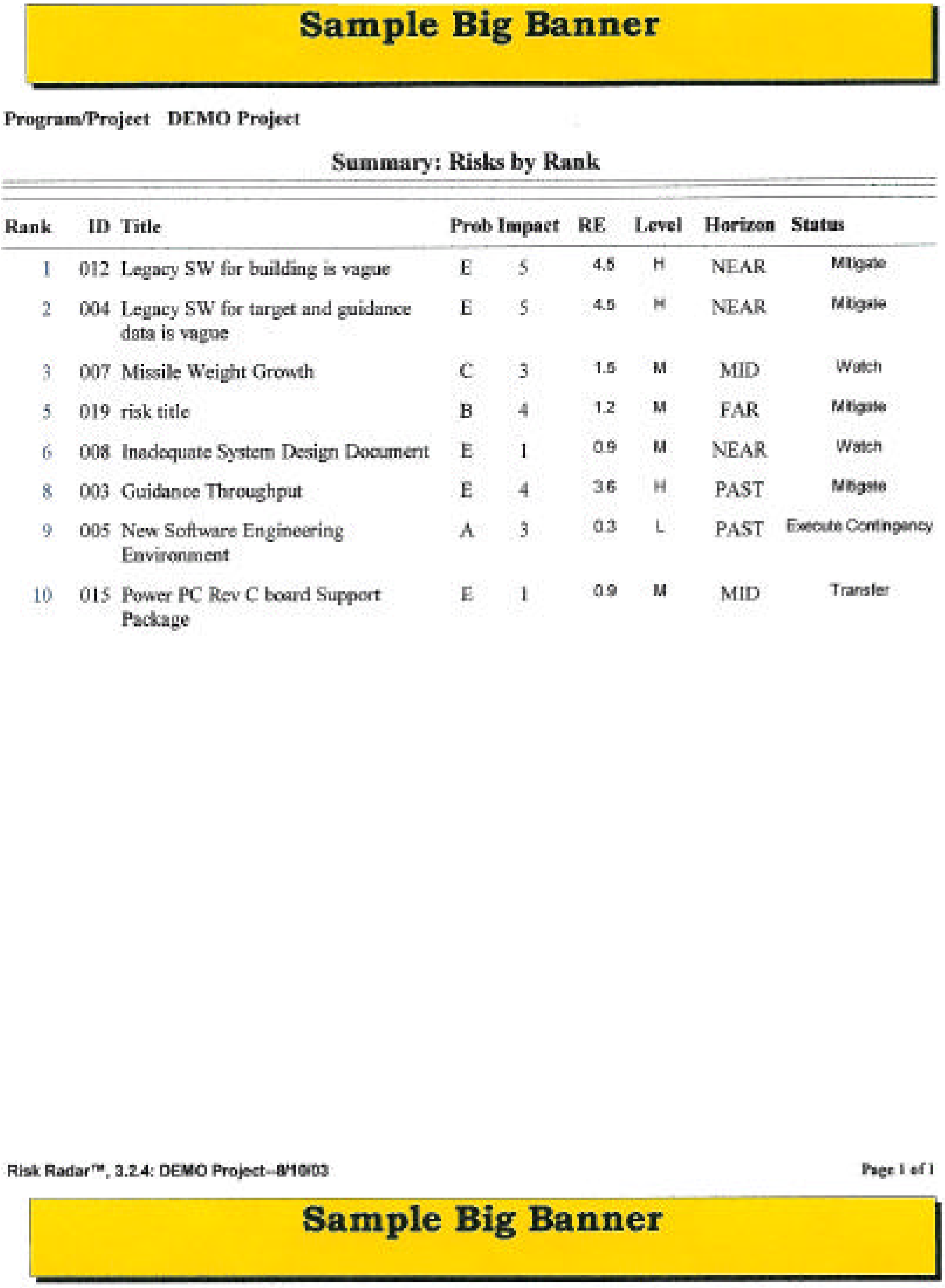
Quarterly Project Status Meetings

Measure: Quarterly project status meetings are held with USAID senior stakeholders and the Office of the Inspector General (IG).

** The Acting CFO has not finalized a schedule to meet with the IG.

Appendix E: Risk Radar Sample Reports

Sample Summary Report



Sample Big Banner

Program/Project DEMO Project

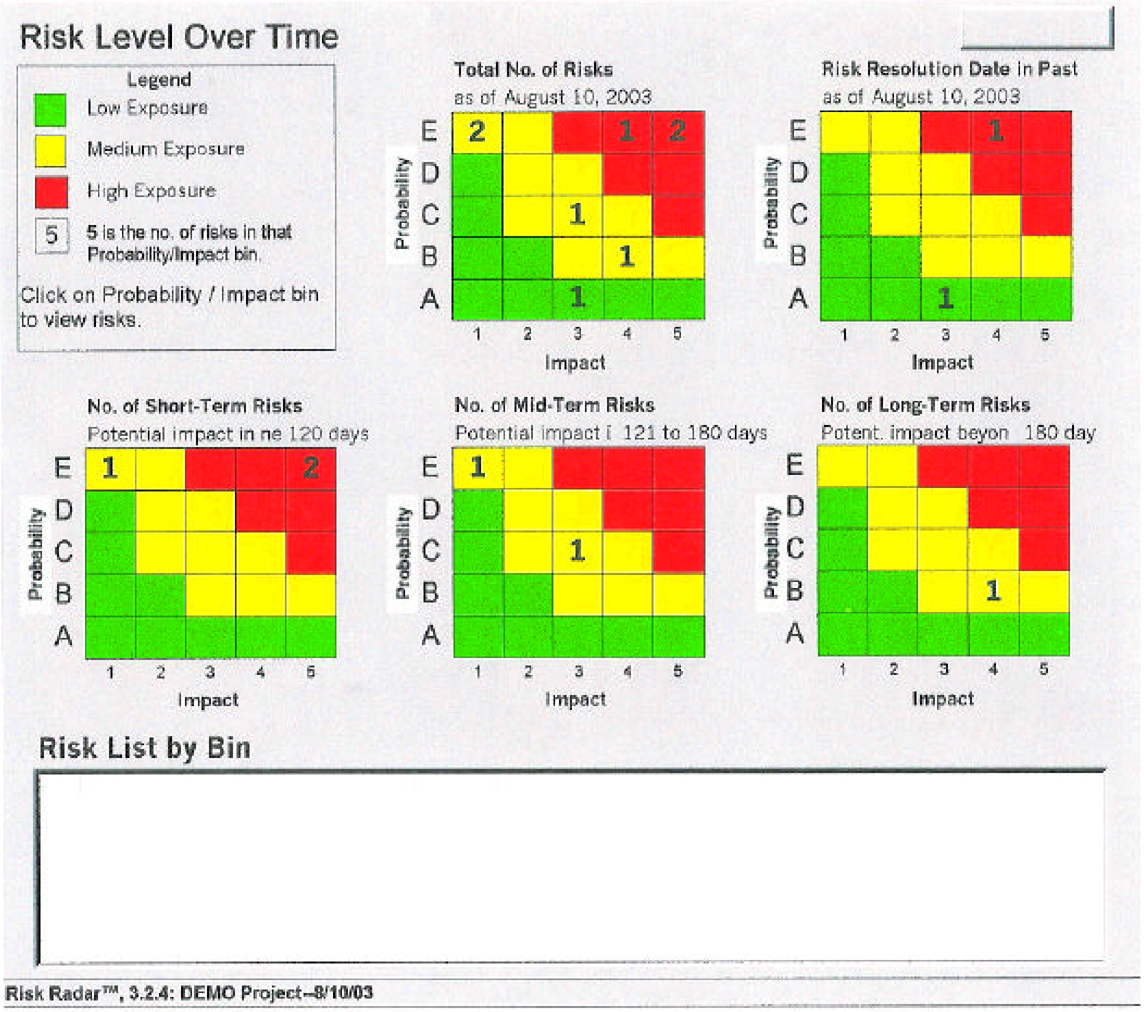
Summary: Risks by Rank

Rank	ID	Title	Prob	Impact	RE	Level	Horizon	Status
1	012	Legacy SW for building is vague	E	5	4.5	H	NEAR	Mitigate
2	004	Legacy SW for target and guidance data is vague	E	5	4.5	H	NEAR	Mitigate
3	007	Missile Weight Growth	C	3	1.5	M	MID	Watch
5	019	risk title	B	4	1.2	M	FAR	Mitigate
6	008	Inadequate System Design Document	E	1	0.9	M	NEAR	Watch
8	003	Guidance Throughput	E	4	3.6	H	PAST	Mitigate
9	005	New Software Engineering Environment	A	3	0.3	L	PAST	Execute Contingency
10	015	Power PC Rev C board Support Package	E	1	0.9	M	MID	Transfer

Risk Radar™, 3.2.4: DEMO Project--8/10/03 Page 1 of 1

Sample Big Banner

Sample Risk Status Report



Risk Level Over Time

Legend

- 🟩 Low Exposure
- 🟨 Medium Exposure
- 🟥 High Exposure
- 5 5 is the no. of risks in that Probability/Impact bin.

Click on Probability / Impact bin to view risks.

Total No. of Risks
as of August 10, 2003

Probability	1	2	3	4	5
E	🟨 2	🟨	🟥	🟥 1	🟥 2
D	🟩	🟨	🟨	🟥	🟥
C	🟩	🟨	🟨 1	🟨	🟥
B	🟩	🟩	🟨	🟨 1	🟨
A	🟩	🟩	🟩 1	🟩	🟩

Impact

Risk Resolution Date in Past
as of August 10, 2003

Probability	1	2	3	4	5
E	🟨	🟨	🟥	🟥 1	🟥
D	🟩	🟨	🟨	🟥	🟥
C	🟩	🟨	🟨	🟨	🟥
B	🟩	🟩	🟨	🟨	🟨
A	🟩	🟩	🟩 1	🟩	🟩

Impact

No. of Short-Term Risks
Potential impact in ne 120 days

Probability	1	2	3	4	5
E	🟨 1	🟨	🟥	🟥	🟥 2
D	🟩	🟨	🟨	🟥	🟥
C	🟩	🟨	🟨	🟨	🟥
B	🟩	🟩	🟨	🟨	🟨
A	🟩	🟩	🟩	🟩	🟩

Impact

No. of Mid-Term Risks
Potential impact i 121 to 180 days

Probability	1	2	3	4	5
E	🟨 1	🟨	🟥	🟥	🟥
D	🟩	🟨	🟨	🟥	🟥
C	🟩	🟨	🟨 1	🟨	🟥
B	🟩	🟩	🟨	🟨	🟨
A	🟩	🟩	🟩	🟩	🟩

Impact

No. of Long-Term Risks
Potent. impact beyon 180 day

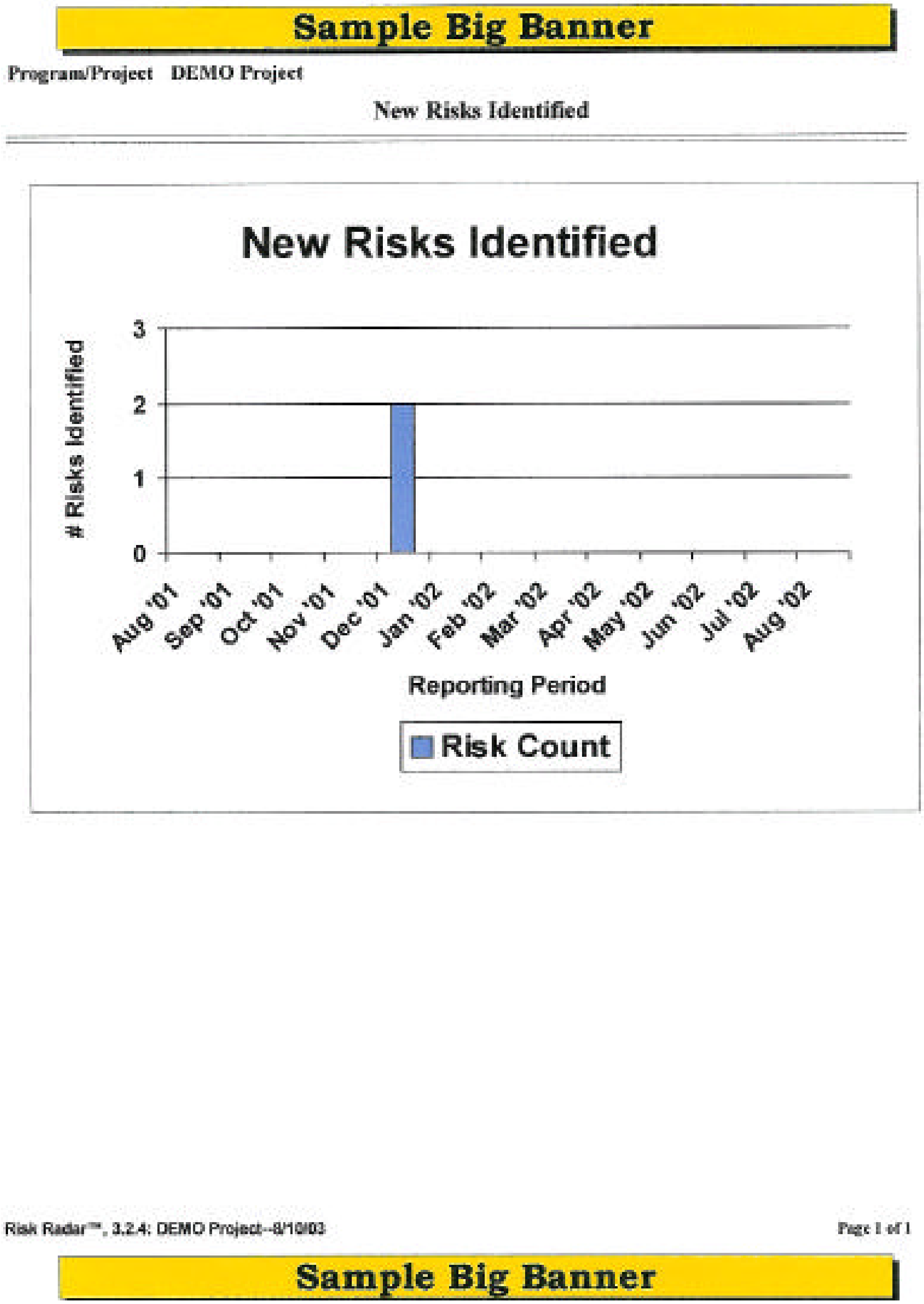
Probability	1	2	3	4	5
E	🟨	🟨	🟥	🟥	🟥
D	🟩	🟨	🟨	🟥	🟥
C	🟩	🟨	🟨	🟨	🟥
B	🟩	🟩	🟨	🟨 1	🟨
A	🟩	🟩	🟩	🟩	🟩

Impact

Risk List by Bin

Risk Radar™, 3.2.4: DEMO Project--8/10/03

Sample Risk Metric Report



Sample Big Banner

Program/Project DEMO Project

New Risks Identified

Risk Radar™, 3.2.4: DEMO Project--8/10/03 Page 1 of 1

Sample Big Banner

Appendix F: Risk Categories

The following risk categories are used in the implementation of the risk management process at enterprise level:

- Business – reliance of congressional and OMB approval of budgets
- Data/Info – replacement cost lost data/information, conversion cost of data/information
- Dependencies and Inter-operability – decisions regarding the BT projects and funding of implementation could impact performance goals
- Feasibility – functional requirements may not be met by baseline software
- Initial Cost – costs for initial deployment may exceed initial forecasts
- Investment Management Capability – program management may not be able to monitor and control schedule, costs, and risks for an investment
- Life-Cycle Costs – life-cycle costs for deployment may exceed initial forecasts
- Monopoly for Future Procurements – locked into a proprietary approach with no alternatives
- Organizational and Change Management – developing and implementing an approach that may require changes in processes, workflows and organizations
- Privacy – unauthorized access to sensitive data
- Project Resources – level of involvement of program management staff for support and availability of subject matter expertise
- Reliability of System – repository tools which may not support technical requirements
- Risk of Project Failure – dynamic requirements from oversight organizations, misunderstanding of capabilities and needs, lack of endorsement, support, and participation from senior management
- Schedule – ability to meet the schedule targets and goals
- Security – unauthorized access to operational systems
- Strategic – OMB or congressional approach and direction that may impact project goals
- Surety – protection of project and program assets
- Technology – consideration of evolving technology and ability to integrate current technology with future platforms
- Technical Obsolescence – technical approach will not evolve to support project or program requirements

Appendix G: Key Participants

Name	Organization	Phone Number
Pat Kristobek	USAID PMO	202-712-1284
Freddy Blunt	USAID PMO	703-465-7172
Kim Hintzman	IBM BCS	703-653-7647
Angela Carrington	IBM BCS	703-465-7055
Jennifer Wilkinson	IBM BCS	703-465-7093
André Armstrong	IBM BCS	703-465-7158

Appendix H: Acronyms List

BT	Business Transformation
BTEC	Business Transformation Executive Committee
CMMI	Capability Maturity Model Integration
CPIC	Capital Planning and Investment Control
EA	Enterprise Architecture
IEEE	Institute of Electronics and Electrical Engineers
PMO	Progam Management Office
PMBOK	Project Management Body of Knowledge
PMS	
QA	Quality Assurance
RML	Risk Management Lead
RMP	Risk Management Plan
USAID	United States Agency for International Development